Gen Docket No. 09-51

Gregory Intoccia

Subject: FW: Workshop

Attachments: Welch Response to Follow Up Questions from 2 October Cyber Security Workshop.docx

Welch Response to
Follow Up Qu...

-----Original Message-----
From: Don Welch [mailto:don.welch@merit.edu]
Sent: Tuesday, October 20, 2009 3:45 PM
To: Joy Ragsdale
Subject: Re: FCC Cyber Security Workshop-Follow-up

Joy,
Attached is my response. It was written in an informal style. Let me know if this is not what you need. Thank you again for the opportunity to contribute.
Don

Donald J. Welch, Ph.D.

President and CEO

Merit Network, Inc.

www.merit.edu

734-527-5701

Connecting Organizations - Building Community

Merit Services Seminar

Oct 29, 2009

http://www.merit.edu/events/archive/specialevents/services2009/

Internet2 IPv6 Workshop

Nov 11, 2009 - Nov 13, 2009

http://www.merit.edu/events/archive/specialevents/ipv62009/

SANS Secure Coding in Java/JEE: Developing Defensible Applications

Jan 5, 2010 - Jan 8, 2010

http://www.merit.edu/events/archive/specialevents/sans541/

Joy Ragsdale wrote:

> Mr. Welch
>
> In order to ensure we have a more complete record, we would appreciate
> your comments in response to the attached questions by November 1, 2009.

> Thank you
>
> Joy M. Ragsdale, Attorney
>
> FCC, Public Safety & Homeland Security
>
> Policy Division
>
> w) 202-418-1697
>
> //
>
> /*** Non-Public: For Internal Use Only ***/
>
> / /
>
> / /
>
> / /
>
> //
>

Welch Response to Follow Up Questions from 2 October Cyber Security Workshop

I would first like to set a context for my responses. My responses pertain to network providers only. I do not think that the network is the place to address most security issues. This comes from both practical and policy reasons. Within the network, much of the context is missing which makes effective security difficult. On the policy side, the techniques necessary to increase security can be misused, and the effort to protect against misuse would consume resources that would probably be better applied to other means. My responses pertain primarily to the security of the network infrastructure.

The next part of my context is the security goals. In some cases these goals can work against each other, so it is not proper to consider security as a single goal. In the most basic sense, security goals are classified as confidentially, integrity and availability. Normally, security efforts are complementary, but not always. It is important to understand the trade-offs and prioritize the goals when implementing a security action. A good example is the use of a stateful firewall in front of an e-commerce site. The firewall may protect confidentiality and integrity, but it can be a very vulnerable target in a denial of service attack thus working against availability.

Finally, it is important to understand the nature of the threat. Once again, security measures that protect against one type of threat may result in greater exposure to another. For example, using very prevalent software may expose you to many attacks by unsophisticated attackers whose main motivation is notoriety. Switching to a little known, or proprietary software may result in far fewer attacks, but may then expose you to much more devastating breaches. Essentially, with little known software, there are fewer attackers publishing fewer exploits. Zero-Day exploits can exist for much longer periods without being patched, because they are only known by the sophisticated attackers who find value holding a exploit until they can gain the maximum advantage.

Responses

I believe that the key to greater security lies in the business case. Since investments in security currently pay off in the avoidance of costs rather than in ways that are easier to quantify, the value of security must lead executives to justify the investment. This value could come from fines, bad publicity, security posture marketing or something that more directly and regularly effects the bottom line of an enterprise. The difficulty is in not only choosing the mechanism, but in keeping that mechanism up to date. For example, say the FCC establishes a set of best practices that a provider had to meet to claim a security level. They would want to do this for marketing purposes. This might be a useful way to get providers to invest in security, but the threat and underlying technology change so quickly that one of two scenarios would dominate. The customers and providers would not value the rating because it would most likely trail current state of the art. Another possibility is that the rating is valued, but doesn't actually do much for the true security posture giving everyone a false sense of security. I don't know what the right incentive would be but it must motivate real increases in security, and balance flexibility, usability, and cost with security.

I think that mandating results is what is required. If a provider is going to provide network services to other entities, it should need the blessing of a central agency. This license should be withdrawn for organizations that do not disclose in accordance with federal regulation. Whistleblower protections would have to be in place as they are for other federal regulations. The difficult question is your next one.

Yes there should. It should not be limited to incidents with global ramifications. If we are going to be successful, we cannot just react to major incidents. We must understand exactly what is happening and be proactive. This requires awareness, which requires a much more data on incidents so that we can understand trends.

Yes, there should be a threshold. The establishment of the threshold, the definition, etc. should be developed with significant input from the community of providers. The North American Network Operators Group, Internet Engineering Task Force among others should have significant input. The important point here is that the network infrastructure is only a small part of the problem. Trying to stop serious attacks on end-user sites in the network cloud is very difficult and fraught with challenges. There are architectural and technology changes that can help end-users with security, but they can't stop the attacks.

It must be a high priority to protect proprietary information. The FCC must have a thorough understanding of what it allows as proprietary information and what it does not. Individual organizations vary widely in what they will share and what they will not. A level and well understood playing field is key to the success of any effort in this area. The challenge is that if security is a marketing advantage, then any attack information becomes valuable. Incentives will probably not work, so regulations will have to be used.

The minimum ROI would be positive, but I do not believe this would be enough. Different organizations may have different threshold ROIs for projects based on their appetite for risk and access to resources. Remember that a security investment does not stand on its own; it competes with other investments for resources. So an additional security analyst may be competing with an additional sales staff. An organization will have to see a greater cost avoidance (or gain) from the security analyst than they would from the sales staff. Estimating the cost of a low probability security incident is difficult and will widely vary.

With respect to integrity check or authorization, it is unclear how you mean these to apply to networks. I'll take a guess. With respect to integrity checks, putting this technology in the network infrastructure will be expensive. So there would have to be an ROI. Customers would have to demand it or be willing to pay more for the service. For example if all health care information could only travel on a network with integrity checking, those health care organizations would be willing to pay for the service and providers would invest in making it happen as a business opportunity. By authentication systems, I assume you mean an architecture where network devices would use authentication (PKI?) to establish the identity and authorization of the next device on the path. This is a significant change to the current architecture that would require major investments by the providers. A business case for the deployment would work, but it would partition the Internet during the transition phase.

The second part of this question, is really another question altogether. I strongly believe that the government should be promoting results rather than actions. There are lots of different ways to make network infrastructure more secure. Prescribing specific actions for all organizations will not result in the most effective security or efficient use of resources. Diverse paths are the best protection against physical threats to a network. Mandating them may put small providers out of business or cause large providers to withdraw from remote areas. Since physical attacks are rare and more risky, providers in remote areas may prefer to take other steps to handle denial of service attacks that keep providers in business and provide a well understood and reasonable level of protection. If there are consequences to failure, eventually most providers will make good decisions.

The national alerting systems must have accurate and timely access information. They must be able to quickly disseminate information and have standard well-understood definitions of proprietary and non-proprietary information.

There needs to be a framework for the collection, analysis and dissemination of security information. For completeness, I'll repeat that disclosure must be mandatory. It must also include the pertinent information. The pertinent information must be pre-balanced between information the companies wish to keep propriety and the information needed for effective action. The FCC needs bring representatives of the network community together and begin negotiation of what constitutes a reportable security incident and the information included in the report. The framework should be as flat as possible. Ideally, state agencies would not be part of the framework. Most networks operate in multiple states and as difficult as the reporting-dissemination process would be to establish, adding more links in the chain would make it harder.

The main processes are the development and dissemination of best practices throughout the community. This happens through formal and informal training, communities of practice, web resources, etc. It is informal, but for those that invest in security, they generally see a return in line with the resources they put into security.

I don't think that ISPs can do much. If we changed the underlying principles of networking to be inconsistent with our national values, there are things we could do and if there was the incentive, new techniques and technologies would emerge. However, this would be roughly akin to changing our road infrastructure to combat criminals that traverse our roads in committing crimes. The cost would be great in freedom, innovation, and privacy as well as monetary.

Hashing is useful for integrity checking. It is only useful, if it is combined with an infrastructure that reliably established the identity and authorizations of all nodes on the network. Otherwise the integrity is easily defeated by the "man-in-the-middle" type attack. Encryption can be useful, but once again it must be part of a larger infrastructure. Where the payload is encrypted and decrypted makes a big difference. Since most breaches occur on the server, encrypted payloads don't help. Encrypted payloads are always combined with integrity checks, but without a secure infrastructure defeating the combination is not difficult. RSA Token Authentication in end-to-end systems is useful but must be part of a larger system. When looking at specific techniques it is useful to understand that security is a system. Each technique by itself can be defeated. By setting up a defense in breadth (can't go around it) and depth (multiple security mechanisms must be defeated), you make the cost in time, money and effort required to breach the system higher. You cannot completely secure a system, you can only increase the cost to do so. Keeping in mind that the systems defense must always be balanced between usefulness, cost and security against a thinking adversary that learns and adjusts very quickly it is very difficult to prescribe specific techniques or technologies to any effect.

Another important rule to remember is that if you breach a layer in the OSI network model, it is much easier to penetrate security at all layers above. Hence encrypting layer 3 payloads fails when an attacker has breached the security at the data link layer (layer 2).

Complicated and diverse supply chains have made the world more and less vulnerable. To attack a single company or industry, an attacker must attack more targets each with different defenses. This is a much more difficult task. However, the payoff is much higher than it had been. Most well run companies have leaner supply chains and a successful attack would have to be sustained for a much shorter duration to be effective. For world commerce to thrive, network communications must interact globally. Therefore, any increase in security will come from a global effort. As difficult as the problem is for the U.S., including the rest of the world adds significantly to the difficulty. Remember the need for defense in breadth and depth. The attackers will seek the weakest point. If implemented properly it could provide the U.S. a competitive advantage in the global marketplace.

Are commercial providers doing enough right now? This is a very subjective question. Network providers currently have enough customers to stay in business. Providers that offer better security appear to have no competitive advantage over those that don't. So I would say that marketplace thinks network providers are doing enough. As evidence, natural events and human error still far outweigh malicious activity when looking at network problems. If end-users had a greater need from network providers for security, the providers would react.

Federal Communications Commission
Washington, D.C. 20554

October 7, 2009

Don Welch, CEO & President
Merit Network, Inc.
1000 Oakbrook Drive
Suite 200
Ann Arbor, MI 48104

Re: National Broadband Plan Proceeding, Docket No. 09-51

Dear Mr. Welch:

Thank you, very much for your participation in the FCC's October 2, 2009 Cyber Security Workshop. The Workshop was very enlightening and provided important information that will be considered in developing a National Broadband Plan.

As a follow-up to the workshop and in order to ensure we have a complete record, we would appreciate it if you could provide your comments in response to the following questions by November 1, 2009 we would appreciate it. Of course, your answers will be made part of the public record for the Broadband Plan proceeding.

Questions

- What would motivate more network providers to adopt approaches to improve security when effectiveness depends on what other providers do, as might be the case with authentication, routing security, and DNS security? Are there policies that the U.S. government should consider in the broadband plan to encourage this?
- With respect to information sharing about outcomes and results, what incentives are needed to encourage service providers to report more data about the occurrence and resolution of cyber security incidents to their customers, the FCC, other government or security-focused agencies, and competitive service providers?
- Should there be a uniform or baseline definition of a "cyber security incident" that mandates when service providers report to their customers, the FCC, other government or security-focused agencies, and competitive service providers a security incident that may be global affecting?
- Should there be a mandatory threshold of affected systems or networks by cyber incidents at which providers must report information to the FCC and other government agencies such as US-CERT and the National Coordination Center (NCC)?

- Should US-CERT, the NCC and any other government-supported entity that receives such information, adhere to confidentiality agreements with commercial providers to allay concerns about the disclosure of competitive market data and proprietary information?

- In regards to the discussion about the adoption of security best practices or standards, please identify the minimum return on investment (ROI) that would encourage commercial service providers to adopt best practices?

- What are some ways that government can encourage industry to promote the increased use of integrity check or authentication systems? What metrics, measures or tools can be used to measure whether an organization can sustain its security practices in times of crisis?

- How can national alerting systems be more effectively utilized to report occurrences and resolutions of cyber security incidents to their customers, the FCC, other government or security-focused agencies, and competitive service providers?

- What ways can state and federal agencies and organizations work together to develop a uniform set of standards for identifying, analyzing, resolving and reporting cyber attack incidents to their customers, the FCC, other government or security-focused agencies, and competitive service providers?

- What are the processes that are being put in place to take into consideration the convergence of technologies and security threats at the same time?

- What could ISPs do to offer their subscribers more security to protect end users intellectual property and data integrity and compromise from cyber thieves that may gain access to this information using keyloggers, IP masking or other virtual means to access the end users data?

- Would it be possible to implement hashing, 256 or 512 Bit encryption, sha 64+1, RSA Token Authentication to ensure the protection of the end users data?

- How have more complicated supply chains from diverse sources, including from outside the United States, introduced vulnerabilities into information and/or network technologies and affected cyber security? Are commercial service providers adequately addressing any such vulnerabilities and, if not, what can be done to better address these concerns?

Thank you once again. Your contribution will help us shape a bold and innovative vision for how we can develop initiatives to strengthen our nation's broadband networks from potentially damaging and global affecting cyber attacks. If you have any questions or comments please feel free to contact me at (202) 418-3619 at your convenience.

Sincerely,

Jennifer A. Manner
Deputy Chief
Public Safety and Homeland Security Bureau
Jennifer.Manner@fcc.gov